Opening Statement of the Honorable Michael C. Burgess, M.D.
Subcommittee on Digital Commerce and Consumer Protection
Oversight of Equifax Data Breach
October 3, 2017

Today the DCCP subcommittee will focus on a massive data breach executed against Equifax, but this is just one of many recent data breaches nationwide. Millions of consumer data, including personally identifiable information, have been compromised leaving customers vulnerable to criminal entities operating mostly on the dark web. In addition, Equifax did not notify consumers until 40 days after observing suspicious traffic and shutting down the source of this traffic.

In an effort to quickly respond to consumers, Equifax's website and call centers were overwhelmed and initially unable to inform individuals if their information had been compromised. Another frustrating factor was the inclusion of a mandatory arbitration clause in the terms and conditions of credit monitoring services being offered, but I understand this has since been removed.

The issue of data breach notification has been before this subcommittee for many years. There is a history of bipartisan cooperation, indicating a strong desire to get this right for all consumers. At this point, there is likely not a single Member of Congress who has not had a constituent, or themselves, affected by a data breach or cyber attack. Without a reasonable federal standard on data security and breach notification, companies are implementing various security protocols and hoping they don't become the next victim of a breach. The lack of a single, federal standard has led to numerous state laws, but data breaches transcend physical boundaries.

Last Congress, this subcommittee passed the Data Security and Breach Notification Act, which would have required breach notification to customers within 30 days, including ways to inquire with the company as well as how to contact the Federal Trade Commission. Companies also had to alert customers that reasonable measures were taken to restore the integrity, security and confidentiality of the data system.

One of the most important sections of the bill would have required entities to implement and maintain reasonable security measures and practices appropriate to the size and type of entity, as well as protect personal information against unauthorized access. These reasonable measures are based on industry accepted practices while remaining flexible to allow advancement in accordance with the security technology market. Currently, such measures might include 2-factor authentication as well as immediate patching of known software vulnerabilities. According to Mr. Smith's testimony, the flaw used to perpetrate the Equifax breach was a known security vulnerability that had an existing patch.

Had the Data Security and Breach Notification bill passed out of this committee with bipartisan support, it may well have become law and prevented, or at least softened the blow of, a data breach on the massive scale experienced by Equifax.

As we work through what happened and how consumers can recover their data security, I hope we can again find bipartisan consensus on data security and breach notification going forward.